Journal of Algebra **227,** 499–503 (2000)
doi:10.1006/jabr.1999.8097, available online at http://www.idealibrary.com on IDEAL®

Symplectic Groups as Galois Groups

Nicholas F. J. Inglis

Department of Mathematics and Statistics, Sultan Qaboos University, P.O. Box 36.

Communicated by Jan Saxl

Received July 2, 1999

1. INTRODUCTION

Let $\mathbb{F}$ be a field containing the field of order q, let x and t be indeterminates, let m be an integer greater than 1, and let

$$\hat{f}(Y) = Y^{q^{2m}} + t^q Y^{q^{m+1}} + xY^{q^m} + tY^{q^{m-1}} + Y.$$

In [3], it was shown that, for $m > 2$, the Galois group of $\hat{f}(Y)$ over $\mathbb{F}(x, t)$ is the symplectic group $Sp(2m, q)$ in its natural action on vectors, and in [4] this was extended to $m = 2$. In this paper we show that much the same is true if we set $t = 1$; if

$$f(Y) = Y^{q^{2m}} + Y^{q^{m+1}} + xY^{q^m} + Y^{q^{m-1}} + Y$$

and $m > 3$, then the Galois group of $f(Y)$ over $\mathbb{F}(x)$ is the symplectic group $Sp(2m, q)$ in its natural action on vectors.

2. q-LINEAR POLYNOMIALS

Let G be the Galois group of $f(Y)$ over $\mathbb{F}(x)$, let $\mathbb{E}$ be a splitting field for $f(Y)$ over $\mathbb{F}(x)$, and let V be the set of roots of $f(Y)$ in $\mathbb{E}$.

LEMMA 2.1. *For $m > 1$, the Galois group G of $f(Y)$ over $\mathbb{F}(x)$ is a subgroup of $Sp(2m, q)$ in its natural action on vectors.*

Proof. First we observe that each term in $f(Y)$ is a multiple of Y raised to a power of q. It follows that $f(Y)$ is q-linear, in the sense that $f(\alpha Y + \beta Z) = \alpha f(Y) + \beta f(Z)$ for all $\alpha, \beta \in \mathbb{F}_q$. Moreover, the coeffi-

0021-8693/00 $35.00

cient of Y is nonzero, and therefore V is a vector space of dimension $2m$ over $\mathbb{F}_q$ and G is a subgroup of $GL(V)$ in its natural action (cf. [1, 8]).

Consider the bivariate polynomial

$$g(Y,Z) = (YZ^{q^m} - Y^{q^m}Z)^{q^{m-1}} + \cdots + (YZ^{q^m} - Y^{q^m}Z)^q + (YZ^{q^m} - Y^{q^m}Z) + (Y^{q^{m-1}}Z^{q^m} - Y^{q^m}Z^{q^{m-1}}).$$

This is q-linear in both Y and Z and $g(Y,Y) = 0$, so that under evaluation g induces an alternating $\mathbb{F}_q$-bilinear map from $\mathbb{E} \times \mathbb{E} \to \mathbb{E}$. We can show that this restricts to an alternating $\mathbb{F}_q$ bilinear map from $V \times V \to \mathbb{F}_q$ by using Abhyankar's Mantra [2]:

$$\begin{aligned}
g(Y,Z)^q - g(Y,Z) &= (YZ^{q^m} - Y^{q^m}Z)^{q^m} + \cdots + (YZ^{q^m} - Y^{q^m}Z)^q \\
&\quad + (Y^{q^{m-1}}Z^{q^m} - Y^{q^m}Z^{q^{m-1}})^q \\
&\quad - (YZ^{q^m} - Y^{q^m}Z)^{q^{m-1}} - \cdots - (YZ^{q^m} - Y^{q^m}Z) \\
&\quad - (Y^{q^{m-1}}Z^{q^m} - Y^{q^m}Z^{q^{m-1}}) \\
&= (YZ^{q^m} - Y^{q^m}Z)^{q^m} - (YZ^{q^m} - Y^{q^m}Z) + (Y^{q^{m-1}}Z^{q^m} - Y^{q^m}Z^{q^{m-1}})^q \\
&\quad - (Y^{q^{m-1}}Z^{q^m} - Y^{q^m}Z^{q^{m-1}}).
\end{aligned}$$

Now

$$\begin{aligned}
Y^{q^m}f(Z) - f(Y)Z^{q^m} &= Y^{q^m}Z^{q^{2m}} - Y^{q^{2m}}Z^{q^m} + Y^{q^m}Z^{q^{m+1}} - Y^{q^{m+1}}Z^{q^m} + Y^{q^m}Z^{q^{m-1}} \\
&\quad - Y^{q^{m-1}}Z^{q^m} + Y^{q^m}Z - YZ^{q^m} \\
&= (YZ^{q^m} - Y^{q^m}Z)^{q^m} + (Y^{q^{m-1}}Z^{q^m} - Y^{q^m}Z^{q^{m-1}})^q \\
&\quad - (Y^{q^{m-1}}Z^{q^m} - Y^{q^m}Z^{q^{m-1}}) - (YZ^{q^m} - Y^{q^m}Z) \\
&= g(Y,Z)^q - g(Y,Z).
\end{aligned}$$

It follows that whenever $y, z \in V$ we have $g(y,z)^q - g(y,z) = 0$, so that $g(y,z) \in \mathbb{F}_q$. Therefore under evaluation g induces an alternating $\mathbb{F}_q$ bilinear map from $V \times V \to \mathbb{F}_q$.

Suppose that $y \in V$ and that $g(y,z) = 0$ for all $z \in V$. Then $g(y,z)$ must be a multiple of $f(Z)$. But the Z-degree of g is less than that of f, so $g(y,Z)$ must be the zero polynomial. Now the coefficient of $Z^{q^{2m-1}}$ in $g(y,Z)$ is y^{q^m}, so we must have $y = 0$. We conclude that the bilinear form induced by g on V is nonsingular.

Finally, we observe that the coefficients of $g(Y, Z)$ lie in $\mathbb{F}_q$, which is a subfield of the fixed field $\mathbb{F}(x)$ of G, so that

$$G \leq \{h \in GL(V) : g(uh, vh) = g(u, v) \forall u, v \in V\} = Sp(2m, q).$$

∎

The following lemma is based on similar results of Abhyankar (e.g., [1]).

LEMMA 2.2. *For $m \geq 1$, the Galois group G of $f(Y)$ over $\mathbb{F}(x)$ is transitive on $V \setminus \{0\}$.*

Proof. This amounts to showing that $Y^{-1}f(Y)$ is irreducible over $\mathbb{F}(x)$. Let

$$\begin{aligned} h(x, Y) &= Y^{-1}F(Y) = Y^{q^{2m}-1} + Y^{q^{m+1}-1} + xY^{q^m-1} + Y^{q^{m-1}-1} + 1 \\ &= Y^{q^m-1}x + \left(Y^{q^{2m}-1} + Y^{q^{m+1}-1} + Y^{q^{m-1}-1} + 1\right). \end{aligned}$$

Now h is linear in x, so it is irreducible as an element of $\mathbb{F}(Y)[x]$, and it has content 1 as a polynomial in x over $\mathbb{F}[Y]$, so by Gauss' Lemma it is irreducible as an element of $\mathbb{F}[Y][x] = \mathbb{F}[x, Y] = \mathbb{F}[x][Y]$. Therefore by Gauss' Lemma it is irreducible as an element of $\mathbb{F}(x)[Y]$; hence G is transitive on $V \setminus \{0\}$. ∎

3. IMPRIMITIVITY

We have seen that G is a subgroup of $Sp(2m, q)$, which acts transitively on nonzero vectors. To show that $G = Sp(2m, q)$ for $m > 3$, we use Hering's Theorem. The following statement is a paraphrase of that in [7].

THEOREM 3.1 [5, 6]. *Let V be a vector space of dimension n over the field of order q and let G be a subgroup of $GL(V)$ that is transitive on $V \setminus \{0\}$. Then one of the following is true*:

(a) *G lies in one of the following infinite families*:
  (i) $G \leq \Gamma L(1, q^n)$.
  (ii) $SL(a, q^b) \trianglelefteq G \leq \Gamma L(a, q^b)$, *where* $a > 1$ *and* $ab = n$.
  (iii) $Sp(2a, q^b) \trianglelefteq G \leq \Gamma L(2a, q^b)$, *where* $2ab = n$.
  (iv) $G_2(q^b)' \trianglelefteq G \leq \Gamma L(6, q^b)$, *where* $6b = n$ *and q is even*.

(b) *G is one of a small number of further examples with $n \in \{2, 4, 6\}$.*

THEOREM 3.2. *If $m > 3$ then the Galois group G of $f(Y)$ over $\mathbb{F}(x)$ is $Sp(2m, q)$ in its natural action on vectors.*

The main step in the proof consists of eliminating the possibility that G is an extension field subgroup:

LEMMA 3.3. *If $m > 1$ then G is not a subgroup of $\Gamma L(a, q^b)$ for any a, $b \in \mathbb{N}$ with $ab = 2m$ and $1 < b < 2m$.*

Proof. Suppose that $G \leq \Gamma L(a, q^b)$, where $ab = 2m$ and $1 < b < 2m$. Now $\Gamma L(a, q^b)$ and hence G act imprimitively on $V \setminus \{0\}$ with blocks of size $q^b - 1$ (the 1-spaces when V is considered as a vector space of dimension a over $\mathbb{F}_{q^b}$). Let y be a nonzero vector and let B be the corresponding block of imprimitivity. Now the setwise stabilizer G_B lies between G and G_y with $|G_B : G_y| = q^b - 1$, so its fixed field $\mathbb{E}$ lies between $\mathbb{F}(x)$ and the fixed field $\mathbb{F}(x, y)$ of G_y. But $f(y) = 0$, so

$$x = -\frac{y^{q^{2m}} + y^{q^{m+1}} + y^{q^{m-1}} + y}{y^{q^m}}$$

$$= -y^{q^{2m}-q^m} - y^{q^{m+1}-q^m} - y^{q^{m-1}-q^m} - y^{1-q^m} = r(y) \in \mathbb{F}(y),$$

and hence $\mathbb{F}(x, y) = \mathbb{F}(y)$ is a simple transcendental extension of $\mathbb{F}$. It follows from Lüroth's Theorem that $\mathbb{E} = \mathbb{F}(w)$ for some $w \in \mathbb{F}(y)$. Therefore $x = s(w)$ and $w = t(y)$ for some rational functions s and t of degrees $(q^{2m} - 1)/(q^b - 1)$ and $q^b - 1$, respectively, with $s(t(y)) = r(y)$.

The only poles of r are 0 (of order $q^m - 1$) and ∞ (of order $q^{2m} - q^m$). First suppose that $t(\infty) \neq t(0)$, in which case we may assume (if necessary replacing w by a fractional linear transformation $(\alpha w + \beta)/(\gamma w + \delta)$ of itself) that $t(\infty) = \infty$ and $t(0) = 0$. Now the only pole of t must be ∞, so t must be a polynomial, and the only zero of t must be 0, so $t(Y) = Y^{q^b-1}$. This implies that $q^b - 1$ divides all the powers of Y appearing in $r(Y)$. In particular $q^b - 1 \mid q^{m+1} - q^m$, which is impossible, since $b > 1$.

We must therefore have $t(\infty) = t(0)$, and (replacing w if necessary) we may assume that $t(\infty) = t(0) = \infty$. Now ∞ and 0 are the only poles of t, so $t(Y) \in \mathbb{F}[Y, Y^{-1}]$ is a Laurent polynomial, $h(Y)/Y^d$, say, where $\deg h = c$ with $c = q^b - 1 > d$. Moreover, the only pole of s must be ∞, so s is a polynomial of degree $e = (q^{2m} - 1)/(q^b - 1)$. Now the orders of ∞ as a pole of r and $s \circ t$ are $q^m - 1$ and de, so $d = (q^m - 1)/e = (q^b - 1)/(q^m + 1)$. This must be an integer and $b \mid 2m$, so the only possibility is $b = 2m$, which is excluded by hypothesis. ∎

Proof of Theorem 3.2. We have already seen that $G \leq Sp(2m, q)$ is transitive on $V \setminus \{0\}$. We invoke Hering's Theorem and proceed to elimi-

nate all cases except $G = Sp(2m, q)$. Since $m > 3$ we have $\dim V > 7$, so the exceptions in case (b) do not occur.

First consider (a)(i). Now the largest intersection between $Sp(2m, q)$ and a $\Gamma L(1, q^{2m})$ is of order $m(q^m + 1)$. This is strictly smaller than $q^{2m} - 1$, so such a group cannot be transitive on $V \setminus \{0\}$.

In the remaining cases G is a subgroup of $\Gamma L(a, q^b)$, where $ab = 2m$ and $a > 1$. By Lemma 3.3 we must have $b = 1$. In case (a)(iv) this gives $\dim V = 6$, contrary to our hypothesis. In case (a)(ii) this gives $SL(2m, q) \trianglelefteq G$, which is impossible, since $G \leq Sp(2m, q)$ and $m > 1$. We must therefore be in case (a)(iii) with $Sp(2m, q) \trianglelefteq G$. But $G \leq Sp(2m, q)$ so we have equality. ∎

Remark. The proof of Theorem 3.2 relies on the Classification of Finite Simple Groups through its use in Hering's Theorem.

ACKNOWLEDGMENTS

Much of the work for this paper was completed while the author was a Visiting Associate Professor at Purdue University. During this time the author learned a great deal from Prof. S. S. Abhyankar, whose influence pervades this paper.

REFERENCES

1. S. S. Abhyankar, Nice equations for nice groups, *Israel J. Math.* **88** (1994), 1–24.
2. S. S. Abhyankar, Factorizations over finite fields, *in* "Finite Fields and Applications," London Mathematical Society Lecture Note Series, Vol. 233, pp. 1–21, Cambridge Univ. Press, Cambridge, UK, 1996.
3. S. S. Abhyankar, More nice equations for nice groups, *Proc. Amer. Math. Soc.* **124** (1996), 2977–2991.
4. Shreeram S. Abhyankar and Paul A. Loomis, Twice more nice equations for nice groups, to appear.
5. C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order. *Geom. Dedicata* **2** (1974), 425–460.
6. C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order, ii, *J. Algebra* **93** (1985), 151–164.
7. M. W. Liebeck, The affine permutation groups of rank three, *Proc. London Math. Soc. (3)* **54** (1987), 477–516.
8. E. H. Moore, A two-fold generalization of Fermat's theorem, *Bull. Amer. Math. Soc. (N.S.)* **2** (1896), 189–199.